REMARKS

Applicants respectfully request reconsideration of the rejection of this application as examined pursuant to the office action of August 27, 2008. In the office action, Claims 1-5, 8-15, 28-30 and 32-41 were examined. Claims 2 and 28 have been canceled. New Claims 42-46 have been added. Claims 1, 3-5, 8-15, 29-30 and 32-46 are pending after entry of this Amendment.

Claims 1-3, 5, 8-15, 28-30 and 33-41 were rejected under 35 USC § 103(a) as being unpatentable over US published patent application Publication No. 2004/0003285 to Whelan et al. ("Whelan"). Claims 4 and 32 were rejected under 35 USC § 103(a) as being unpatentable over Whelan in combination with US published patent application Publication No. 2003/0046583 to Goldman et al. ("Goldman"). Claim 11 was rejected under 35 USC § 103(a) as being unpatentable over Whelan in combination with US published patent application Publication No. 2004/0111636 to Baffles et al. ("Baffles").

Independent Claims 1 and 30 have been amended to describe the present invention in a manner that markedly distinguishes it from the cited references. Specifically, Claims 1 and 30 have been amended to include the features of: 1) acquiring information, or providing a function to acquire information, about the attached functions seeking access to the network services; 2) determining, or providing a function to determine, whether one or more stored policies exist for the attached functions; 3) allowing, or providing a policy to allow, at least one of the one or more attached functions to access a selectable portion of the network services based on a policy established in one or more of the interconnection devices; and 4) saving, or providing a function to save, changed policies for the attached function or functions. These features distinguish the present invention and are fully supported in the Specification of the present application at least in paragraphs (34)-(38) and at least in paragraphs (26), (27) and (36) of the specification of Application No. 10/629,331, the contents of which has been incorporated in the present Specification by reference.

The inclusion into independent Claims 1 and 30 of language directed to determining the physical or logical address of the source of an intrusion is supported by original Claim 2. The inclusion into independent Claims 1 and 30 of language directed to identifying the one or more interconnection devices is supported by original Claim 1. New Claims 42 and 44 are directed to

connecting the attached functions directly to the interconnection devices. The language used in those claims is fully supported in the Specification at least in FIG. 1. New Claims 43 and 45 are directed to establishing policies for the attached function directly from the interconnection devices without communicating with a centralized server. The language used in those claims is fully supported in the Specification at least in paragraphs (12) and (45). New Claim 46 is directed to including in at least one of the interconnection devices intrusion detection functionality as well as policy changing functionality. The language used in that claim is fully supported in the Specification at least in paragraph (32).

Applicants respectfully submit that the amendments made to the claims are supported by the Specification and clearly distinguish the present invention from the cited references.

The 35 USC § 103(a) rejections

Claims 1-3, 5, 8-15, 28-30 and 33-41 were rejected under 35 USC § 103(a) as being unpatentable Whelan. It is stated in the office action that Whelan teaches establishing and changing signal transfer policies for each of a plurality of interconnection devices. Applicants respectfully suggests that Whelan makes no mention of policies or changing policies as a result of an intrusion. In fact, the word "policy" is not included at all in the Whelan reference. In relation to the operation of a network system, a policy is a guide used to define specified principles. Carrying out a specified policy involves conformance with a set of rules or steps to be performed. A simple analogy may be helpful. An example of a parental policy with respect to a child driving would be "My child is not permitted to drive after 9PM." That policy may be implemented in any of a variety of ways. For example, one parent may take away the keys for the car at 8:59PM., while another parent may lock the car in the garage at 8:59PM. Either way, the established policy is carried out.

In regard to the present invention and the distinction from the Whelan reference, Whalen describes only one policy. That policy is: deny all rogue access points from accessing the network. A variety of mechanisms, or rules, are proposed for carrying out that policy, such as changing the MAC filter settings, blocking all wireless communications over a specified period of time, or isolating the rogue device. In all instances, the policy has not changed, just the particular rules. Therefore, Whelan does not establish policies. That has already been done. Further, Whelan does not change policies based on intrusion detection. Instead, Whelan simply

notes that certain specific steps--rules--are to be carried out upon making the detection. The policy, however, does not change. Still further, Whelan focuses all of the indicated rules on dealing with the particular rogue access point detected--or blocking all access points from accessing the network. Whelan fails to teach sufficiently the desire to view the network as a whole, or the advantage in establishing and changing policies with respect to any attached function or interconnection device to provide the most effective security for the entire network. Whelan's approach may effect a security improvement, but does so without regard to minimizing disruption to the network as a whole.

On the other hand, the present invention provides for complete network security in a very efficient manner. That is, the intrusion is considered and policies are or may be changed to deal granularly with the intrusion rather than in a wide swath (such as the option laid out by Whelan to cut off all wireless communications with the network during a specified time period--blocking good as well as bad actors from accessing the network). This is achieved in the present invention by considering the intrusion, identifying the one or more attached functions and/or interconnection devices that are involved and/or are likely to be involved, and initiating policy changes suitable to address the intrusion detected and/or to anticipate any additional unauthorized activity. That is, the present invention is directed to changing policies, which will result in changes in rules to be carried out by designated interconnection devices. Whelan fails to disclose such methods and functionality.

Applicants also wish to note that Whelan directs any rule changes to be implemented to carry out the single policy of rogue access point isolation through a central control arrangement. Therefore, any change in that policy is generated at and directed from a central location, such as a central policy server. On the other hand, the present invention effects policy changes at one or more of the interconnection devices, as noted in the presently pending independent claims.

Applicants have amended independent Claims 1 and 30 to further distinguish the present invention from Whelan. Specifically, those claims have been amended to describe the method and system as including steps/functions directed to determining whether any stored policies exist for attached functions seeking access to the network system, and to saving changed policies made for the attached functions. Again, these amendments are related to policies for the attached functions, not solely rules. In either case, Whelan fails to disclose in any manner the concept of checking for existing policies--not rules--and saving changes to policies for the attached

functions defined. Whelan simply blocks or isolates rogue access points that are not on a designated list.

Whelan also fails to envision the option of considering network access for such devices seeking access before activating complete access denial. In addition, the present invention considers changing policies for such devices based on intrusion information that may or may not be directly related to such devices. The present invention, as described by the amended independent claims, allows for making policy changes for any interconnection device and any attached function under any condition, including conditions that occur independent of actions carried out by attached functions for whom policy changes may nevertheless be made.

In view of the amendments made to independent Claims 1 and 30 and the arguments presented herein, Applicants respectfully suggest that the 35 USC § 103(a) rejection of Claims 1-3, 5, 8-15, 28-30 and 33-41 based on Whelan has been successfully traversed. Withdrawal of that rejection is therefore requested.

Claims 4 and 32 were rejected under 35 USC § 103(a) as being unpatentable over the combination of Whelan and Goldman. Claims 4 and 32 are dependent claims directed to the concept that specific interconnection devices may change directly their own signal transfer policies. The office action contends that Goldman teaches the same capability, citing paragraphs [003] and [0031] of that reference. Applicants respectfully disagree with that contention. Those paragraphs of the Goldman reference identify security software packages. One of the paragraphs describes a configuration module that may be used to generate such software packages. That same paragraph also notes that such software packages may include or be associated with firewalls, routers, switches, etc. It appears that that particular portion of the Goldman reference is the one relied upon in the office action. Apart from the fact that one of ordinary skill in the art is unlikely to argue a router or switch (which are interconnection devices) can be included in a software package, Applicants respectfully suggest that that statement does not teach the concept of an interconnection device changing directly its own signal transfer policies. Instead, it appears that the Goldman reference teaches a centralized security system in which modifications to policies are established centrally and then distributed to such interconnection devices for implementation of rules associated therewith. Goldman fails to state, and it cannot be fairly

inferred from those paragraphs, that any sort of interconnection device configures its own policy changes without instruction from a centralized controller, such as a centralized policy server.

Applicants further suggest that Goldman fails to teach a method and related system for responding to network system intrusions involving a check for the existence of stored policy histories for attached functions and saving policy changes made for attached functions. In view of the amendments made to independent Claims 1 and 30, the arguments presented with respect to the Whelan reference and the arguments presented here regarding the Goldman reference, Applicants respectfully suggest that the 35 USC § 103(a) rejection of Claims 4 and 32 as being unpatentable over Whelan in combination with Goldman has been successfully traversed. Withdrawal of that rejection is therefore requested.

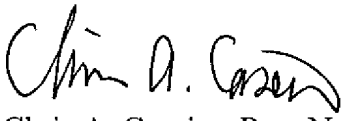
Claim 11 was rejected under 35 USC § 103(a) as being unpatentable over the combination of Whelan and Baffles. Claim 11 is a dependent claim directed to the concept of permitting attached function connectivity for an attached function identified as a source of an intrusion but minimizing its access to network services while it is being analyzed. Applicants note that Baffles fails to disclose a method involving the steps of checking for saved policy history for attached functions and also saving changed policies established in response to a detected intrusion. In view of the amendments made to independent Claim 1, the arguments presented with respect to the Whelan reference and the arguments presented here regarding the Baffles reference, Applicants respectfully suggest that the 35 USC § 103(a) rejection of Claim 11 as being unpatentable over Whelan in combination with Baffles has been successfully traversed. Withdrawal of that rejection is therefore requested.

CONCLUSION

In view of the foregoing amendments made to the claims and the remarks made herein, Applicants respectfully suggest that the rejections under 35 § 103(a) have been successfully traversed. Allowance of pending Claims 1, 3-5, 8-15, 29-30 and 32-46 is therefore requested.

By this amendment, two dependent claims have been canceled and five new dependent claims have been added. Therefore, an additional filing fee for three dependent claims is submitted herewith.

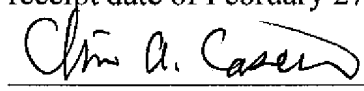
Respectfully submitted,



Chris A. Caseiro, Reg. No. 34,304
Attorney for Applicants
Verrill Dana, LLP
One Portland Square
Portland, ME 04112-0586
Tel. No. 207-253-4530

Certificate of Transmission

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, using the EFS-Web service of the US Patent Office on February 27, 2009. It is hereby requested that this communication be assigned a receipt date of February 27, 2009.



Chris A. Caseiro